ITEA Journal 2009; 30: 111–116

Test and Evaluation Strategies for Network-Enabled Systems

Stephen F. Conley
U.S. Army Evaluation Center, Aberdeen Proving Ground, Maryland

A hierarchical series of strategies is described as an approach for testing and evaluating network enabled systems and systems of systems. The approach builds upon traditional platform performance and requirements-based testing and amplifies it to encompass the additional complexities of interacting systems with their potential for emergent behavior. It is in these interactions that the preponderance of "unknown unknowns" resides and the number of interactions grows geometrically with the size. Future tests will never be able to test a full factorial test matrix. Test and evaluation professionals must develop a systematic approach for building up results from single network nodes to complete joint systems. The hierarchical test strategies, combined with distributed testing and high fidelity live-virtual-constructive environments, are proposed as the most expedient means for satisfying network centric test requirements within time and budget constraints while mitigating technical and programmatic risk.

Key words: Hierarchical test strategies; joint network testing; global information grid; network-enabled systems; Platform as a Network Node (PANN); capability based testing; system-of-systems testing.

Test and evaluation (T&E) has traditionally involved independent platform testing of single entities. Testing is done in a serial fashion: A test would be performed, data gathered, and then the system would move to the next test center. This process is time consuming, inefficient, and insufficient for network-enabled systems. Evaluation would typically be done in a serial fashion with evaluators left to analytically synthesize how well the complete system works by fusing results from multiple test sites under multiple test conditions. For future network-enabled systems like the Future Combat Systems (FCS), however, the integration of systems-within-systems, interoperability, and networking are prime concerns, and testing requirements must be reconsidered.[1] The T&E of network-enabled systems will take new strategies like Platform as a Network Node (PANN), capability-based testing, systems-of-systems testing, and joint network testing.

Introduction

So what defines a network-enabled system? Whether it's a radiac meter sending a nuclear, biological, or chemical report, an FCS command and control vehicle with a battle-staff operating on the move, every system that has a requirement to join the Global Information Grid (GIG) or that has the net-ready key performance parameter as a requirement is a network-enabled system. This means most of the systems being built today are network enabled.

The Defense Information Systems Agency (DISA) is building the GIG as well as developing the Network Enabled Command Capability system and the Network Centric Enterprise Services. In addition, the Test Resource Management Center and the Joint Forces Command (the Joint community) are focusing on network-testing resources. These programs set the stage for understanding why standard methods are required for testing and evaluating network-enabled systems.

To understand how to incorporate these new strategies, we must have a common definition of the "Network." The U.S. Army Training and Doctrine Command and the FCS program have developed the Army definition of a network:

> *"an interconnected, end-to-end set of information capabilities and associated processes that displays,*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Test and Evaluation Strategies for Network-Enabled Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Evaluation Center,Aberdeen Proving Ground,MD,21005**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

disseminates, stores, and manages information on demand to Warfighters, policy makers, and support personnel."[2]

The cornerstone of Department of Defense (DoD) transformation is the ability of future forces to effectively conduct network centric operations in combat and in operations other than war. The Army program driving the need for network-enabled system testing is FCS and the complementary systems supporting it (e.g., the Joint Tactical Radio System, and Warfighter Information Network-Tactical [WIN-T]). For FCS to meet its requirement to test the FCS network, as stated in the National Defense Authorization Act 2008, SEC. 211, there must be an evaluation of the overall operational effectiveness of the FCS network including:

"(a) an evaluation of the FCS network's capability to transmit the volume and classes of data required by Future Combat Systems approved requirements; and (b) an evaluation of the FCS network performance in a degraded condition due to enemy network attack, sophisticated enemy electronic warfare, adverse weather conditions, and terrain variability."[3]

However, the network resides on and will operate on the FCS platforms; manned, unmanned, ground, and aerial. The FCS network therefore must be tested while on these FCS network-enabled systems. In addition, these network-enabled systems are not effective unless the users in the network-enabled systems can access the network and execute their assigned tasks while transmitting and receiving the right information to the right person at the right time in the right format, whether they are static or mobile.

To enable this, testers and evaluators need to incorporate the following strategies: PANN, capability based testing, systems of systems testing, and joint network testing.

PANN

PANN testing is a holistic, network-centric view of testing that enables an understanding of the effects of network-enabling components on the host platform, as well as the effects of the host platform on the network-enabling components as viewed in *Figure 1*. It enables an evaluator to characterize the network node enshrouded in a platform and understand how it will operate as a node of a mobile ad-hoc network. View the platform in PANN testing as a soldier, truck, tank, unmanned ground vehicle, unmanned aerial vehicle, loitering munition, or sensor that may be comprised of

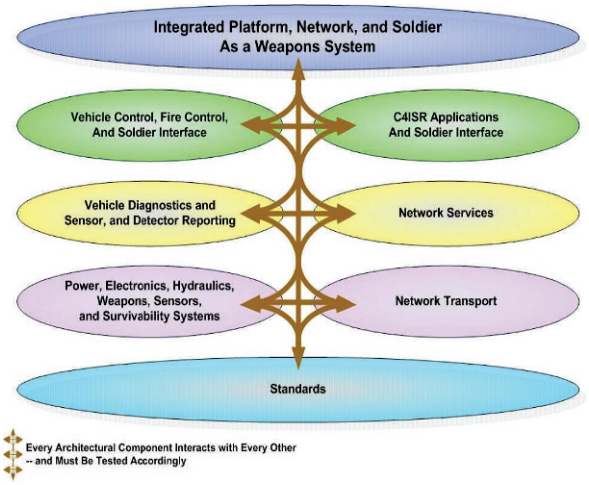


Figure 1. Platform as a network node.

one or multiple communications components or systems that have the ability to send and/or receive data.

PANN will need to incorporate new metrics like WIN-T's communications success rate and information dissemination success rate. It will require a standard for the conduct of data dissemination with a live-virtual-constructive environment; a common synthetic environment that can be used to envelope the prototype in a network located on a virtual test center terrain. PANN will need a standard suite of models and simulations that place the vehicle in an operationally relevant environment including signatures, weather, atmosphere, sensor effects, human effects, digital terrain including natural and manmade terrain representations, full electromagnetic spectrum, soil conditions, virtual battlespace, a communications effects server to emulate not simulate multiple network nodes and traffic, Joint Program Executive Office propagation models, disturbance environments, and a composable next-generation computer-generated force toolset like OneSAF. Services should leverage what DoD has already done. For example, Army testers should not rebuild weapons models; they should use the Army Research, Development, and Engineering Command models. The Army's test centers have almost every terrain a system will encounter. The Army Test and Evaluation Command should focus on the virtual representation of these environments, modeling the terrain to the level of detail that is needed for each variable: weather, atmosphere, obstructions, etc. To develop this correctly, each variable must be built as a service or capability to allow turning the variable on and off as the test conditions dictate. To remain in line with the Joint community, the infrastructure that ties it all together, the middleware, must be test and

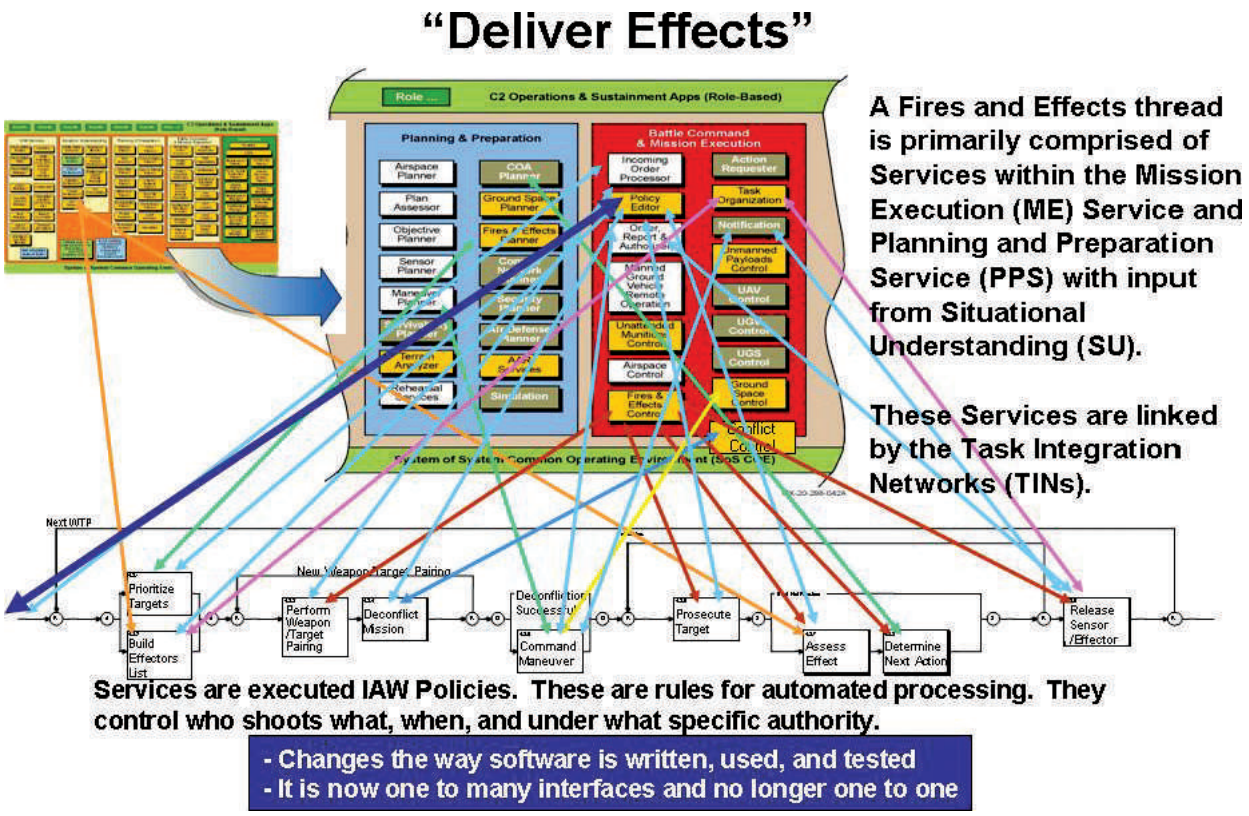


Figure 2. Capabilities based testing.

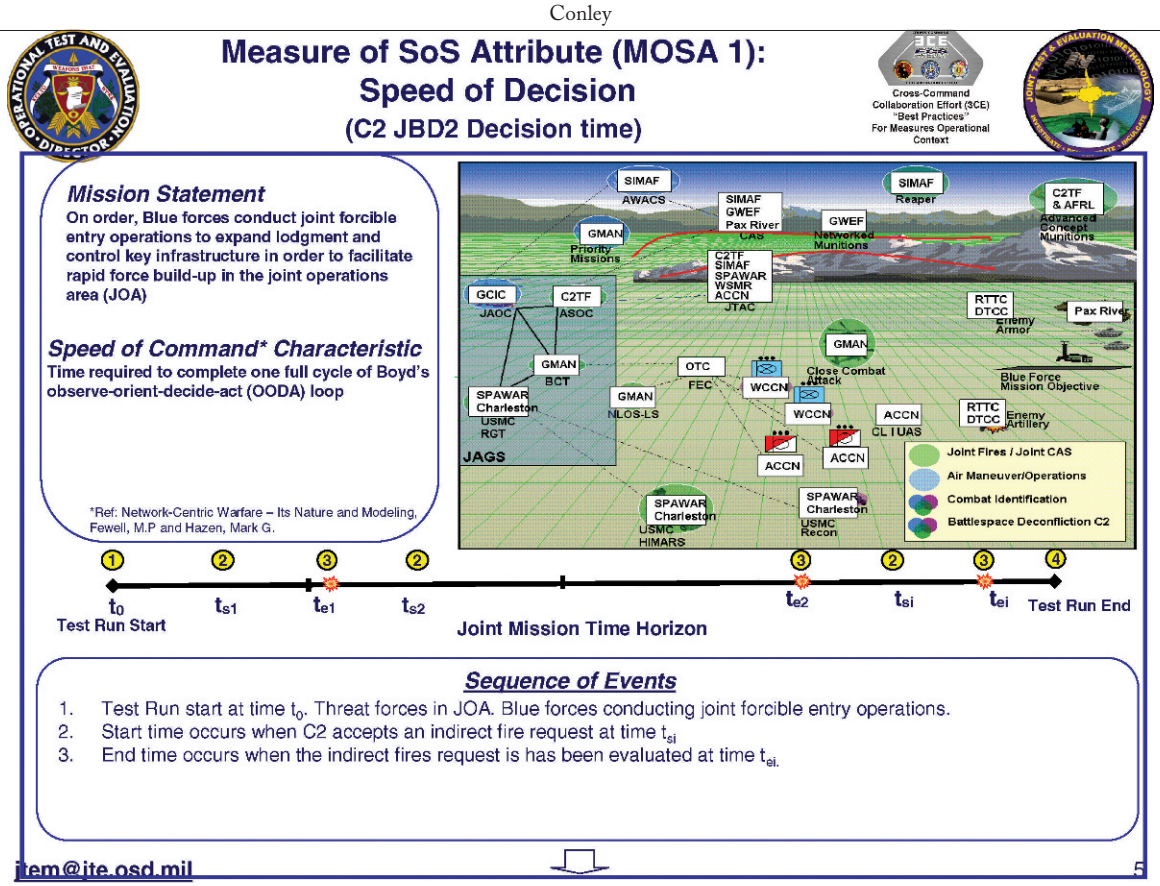
training enabling architecture[4] or at a minimum provide a gateway for high level architecture and distributed interactive simulation protocols. Modeling and simulation must also be portable to a high performance computing (HPC) system, ensuring scalability for T&E. Testers and evaluators must work together to ensure that these models and simulations have gone through the proper verification, validation, and accreditation steps to enable modeling and simulation to be used for evaluation while being executed in developmental testing.[5]

Capabilities Based Testing

Capabilities based testing incorporates the following DoD policy: "Testing and evaluation should begin early, be more operationally realistic, and continue through the entire system life-cycle."[6] Every system—manned, unmanned, aerial, soldier, or sensor—plays a specific role in the overall operation of a military unit and has designated missions. Now that these systems are becoming network-enabled, T&E must include the typical platform and systems tests plus the understanding of how that platform or system will be used and by whom. To evaluate a network-enabled system, we must have an understanding of the tasks that must be performed; the user roles, people, interfaces, and knowledge required to operate the system; an understanding of the application and service layers; and a report that all operate as prescribed and safely. To perform this type of testing, it is imperative to develop a combination of live, virtual, and constructive testing capabilities that enable mission-based tests.

Understanding the tasks and user–operators of a platform enables identification of software functionality and interfaces; addresses conflict of resources in overloaded situations between the platform and its network-enabled components; and can enable measuring the cognitive load of the user. Testers and evaluators must think in terms of vignettes: create the quantity and synchronization of threads that lead to proper network loading; create the unit of soldiers performing individual or collective tasks; and enable the measurement of human cognition and interplay in the network operation. Incorporating vignettes in developmental testing adds robustness to the vignettes planned for operational tests. This effort helps testers and evaluators understand the mission thread and capabilities-based testing. The FCS mission of "deliver effects" provides an excellent example of capabilities-based testing (see *Figure 2*).

Tester and evaluators must understand that network-enabled systems use the network application and



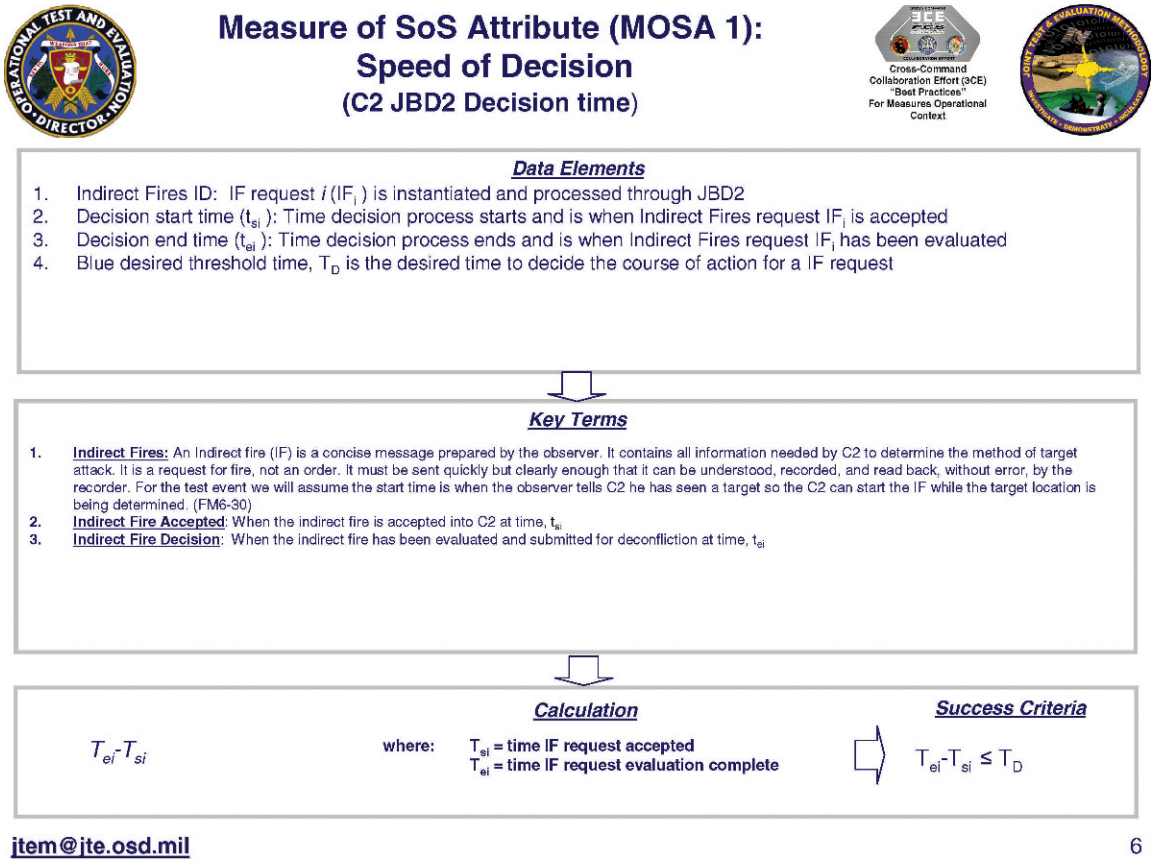


Figure 3. Common measures framework.[7]

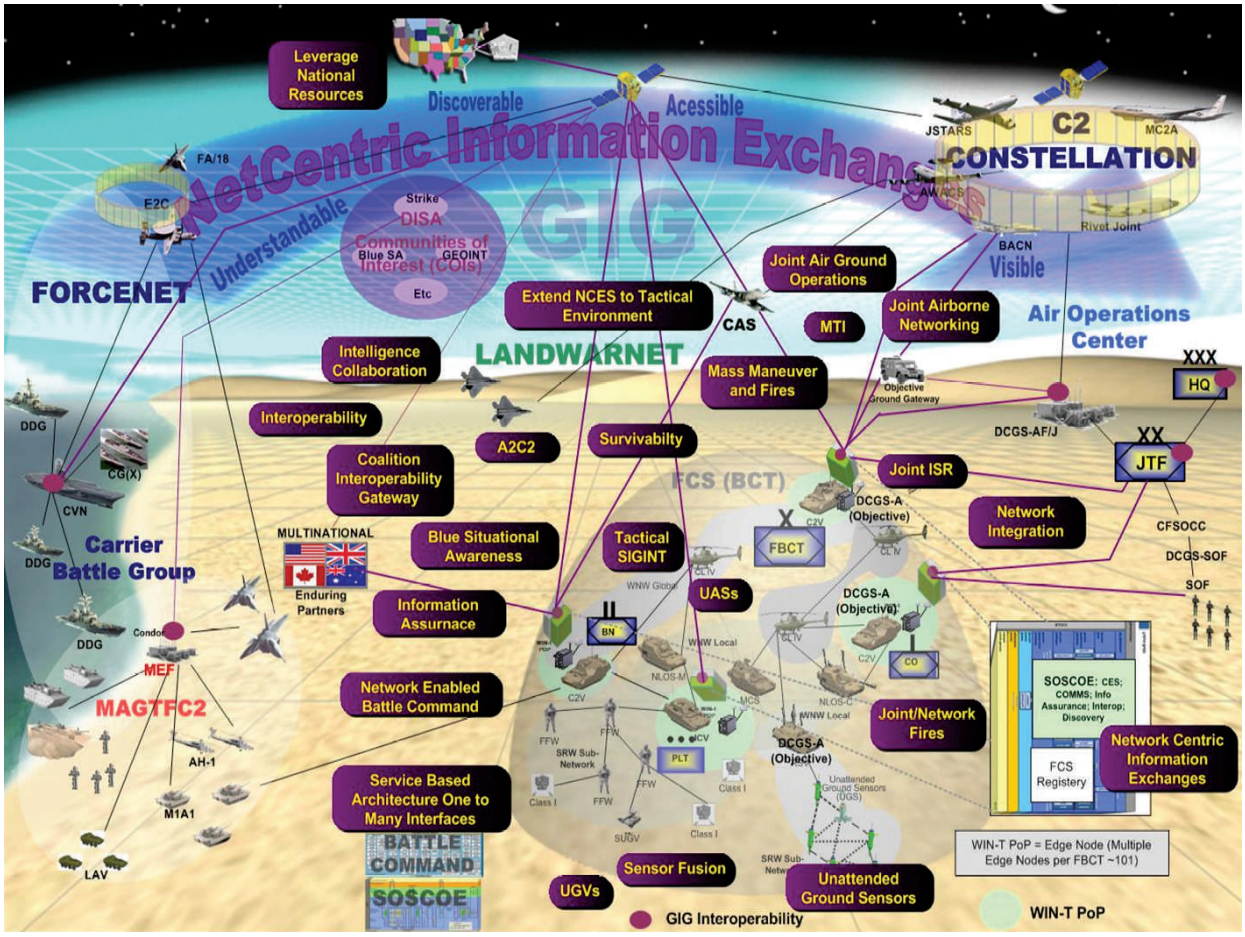


Figure 4. The DoD GIG's NetCentric Information Exchange Environment.

service layers to automate many of the functions currently done by soldiers over voice nets. *Figure 2* shows just that. Each capability has multiple steps, each step has multiple information requirements, and each information requirement is provided from a different source. In the current force these different sources could be information provided by separate staff sections; to enable this automation transition, the application and service layers are being built using a service-oriented architecture (SOA) so the software does the staff coordination, sometimes without human intervention. This software will operate while the host platforms are operating regardless of whether the host is static or mobile.

To complicate matters, to produce a safety release for a platform, testing must ensure the automated processes typically performed by the platform are conducted and that they operate correctly. This requires that testers ensure that the platform software and battle command software operate together safely, under specific conditions, within standards per the missions expected of the platform or system.

Testers and evaluators must place the network under test in a live-virtual-constructive mission environment and exercise the proper threads associated with the platform and its user with a common-measures framework. A common-measures framework enables testers and evaluators to understand what the correct tasks are and what data to collect, both for developmental testing as well as some operational testing.

System-of-systems testing (SoS)

SoS testing looks at a unit conducting a function of a military operation. The U.S. Army Training and Doctrine Command has written 25 integrated processes or unit level mission threads that combat brigades and below must be able to conduct to be effective. The FCS program has further refined these into 12 integrated functional capabilities that describe the specific actions that must take place to facilitate the functioning of a future force brigade combat team. Each of these processes is a set of complex mission threads that incorporates multiple vehicles and personnel executing multiple roles or tasks. To ensure that

a family of systems is ready to conduct an operational test (e.g., limited user test or initial operational test and evaluation), developmental testing ensures that the mission threads operate correctly, and that the SOA applications and services operate correctly, beforehand. The development of a distributed testing capability is a key component to successful system-of-system testing because it enables systems in separate geographical locations to operate together as if they are on the same piece of terrain. An example of such a test actually executed by Joint Test and Evaluation Methodology project and FCS is depicted in *Figure 3*.

Joint network testing

System-of-systems testing enables the final strategy needed to test and evaluate systems for DoD, joint network testing. The end state that DoD is building toward is for all Services to become completely GIG compliant and all Services to be operating in one net-centric information exchange environment as shown in *Figure 4*. To enable joint network testing, it is critical that the Services become involved in joint efforts such as Joint Mission Environment Test Capability, Interoperability T&E Capability, the Joint Test and Evaluation Methodology, and the Army Air Expeditionary Force exercise. Services should actively seek opportunities to operate in large multisite exercises to better prepare for joint network test events. Involvement in these types of exercises enables the maintenance of a persistent test network capability and a current understanding of the evolving net-centric capabilities of acquisition programs. A persistent network is one that can be brought online when needed or one that operates 24 hours a day, 7 days a week, driven by test and evaluation requirements. A persistent network is more than hardware and software. It includes the personnel and their knowledge base to conduct distributed testing. *Figure 4* is a picture of where DoD is going and why services must come together and create a Joint Network testing capability to ensure that all network-enabled systems can operate on the DISA GIG.

Conclusion

DoD is transitioning to network-centric warfare. Programs are building network-enabled systems as part of that transition. The T&E community must transition as well. There are four strategies that the T&E community must embrace to transition to network-enabled T&E, and those strategies are PANN, capabilities-based testing, systems-of-systems testing, and joint network testing. If DoD is to test and evaluate the complex network-enabled systems they are building while meeting the net-ready key performance parameter and ensuring GIG compliance, these are the strategies that must be implemented. Testing and evaluating a platform and then checking the platform's communications systems separately will no longer ensure network-enabled systems are effective, suitable, and survivable. If DoD is to transition to network-centric warfare with network-enabled systems, the T&E community needs to transition as well. ❑

Stephen Conley holds a bachelor's degree in industrial engineering from Lafayette College and a master's of business administration in information systems from City University. He is a retired U.S. Army Signal Corps officer whose last Army tour of duty was with the Army Evaluation Center where he was the Future Combat Systems (FCS) Network Evaluator. In August 2006 he began a second career as an Army civilian working for the U.S. Army Test and Evaluation Command, first as a test technologist in the U.S. Army Developmental Test Command and most recently as a division chief in the Army Evaluation Center's Future Force Evaluation Directorate. As division chief, Mr. Conley leads the evaluation for the Army's Future Combat Systems. E-mail: Stephen.F.Conley@us.army.mil

Endnotes

[1]Simmons, B. M. and J. M. Barton, 2006. Distributed testing: helping the U.S. Army develop a network-centric warfare capability. *ITEA Journal of Test and Evaluation*, 27 (1): 29–34.

[2]FCS Test and Evaluation Master Plan (TEMP), Annex B "FCS Network," page B-1.

[3]House of Representatives Report. 1585-32 Subtitle B-Program Requirements, Restrictions, and Limitations. SEC. 211. Operational Test and Evaluation of Future Combat Systems Network. National Defense Authorization Act for fiscal year 2008. Washington, D.C.: United States House of Representatives.

[4]Test and training enabling architecture development is sponsored by the Central Test & Evaluation Investment Program and supported by the U.S. Joint Forces Command (JFCOM). https://www.tena-sda.org/display/intro/Home.

[5]ATEC Technical Note. Net-Ready Key Performance Parameter (NR KPP), September 2006.

[6]Department of Defense Report to Congress on Policies and Practices for Test and Evaluation on National Defense Authorization Act for FY 2007, Section 231 by Deputy Under Secretary of Defense (Acquisition, Technology, and Logistics), September 18, 2007.

[7]Joint Test and Evaluation Methodology (JTEM) Technical Advisory Group IV, Colonel Eileen Bjorkman, Joint Test Director, September 14, 2007.